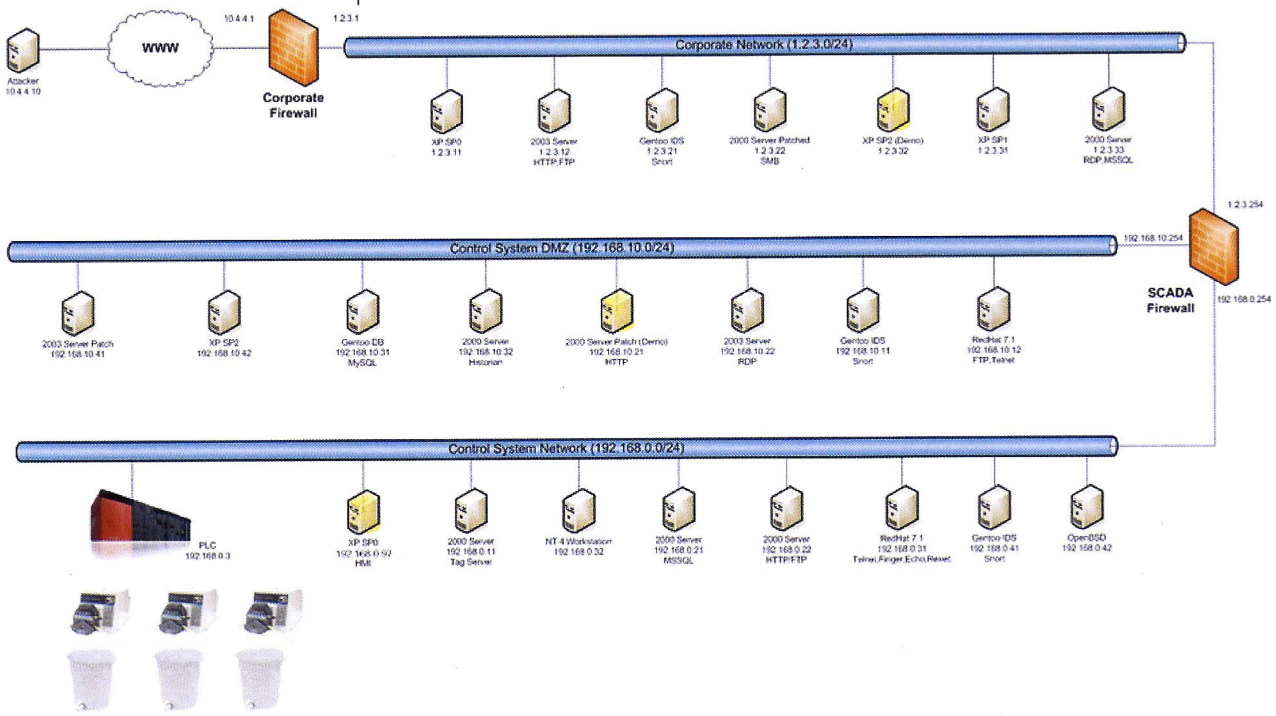
Learning Objective 3

Session 2: Process Control Attack Demonstration

In this session, we will focus on a process control demonstration and then discuss the basic control systems security considerations.

LO3: Discuss the process control exploit demonstration

The demonstration network is representative of one found in industry. The network is segmented into three subnets that include the Corporate Network, the Control System Demilitarized Zone (DMZ), and the Control System or SCADA Network.



Network segmentation is one of the first steps in the "defense-in-depth" strategy, and it helps to localize threats and minimizes the impact on an organization.

Network segmentation benefits:

- Improve network performance and reduce network congestion
- Help contain and prevent attacks from overflowing into other networks
- Improve security by ensuring that nodes are not visible to unauthorized networks
- Reduce the size of broadcast domain.

The **corporate network** includes servers and workstations that would typically be found in a business environment including a Web server, a database server, and several clients. The corporate network is isolated from the control system DMZ and the control system network by a firewall.

The **control system DMZ** includes database servers, company internal web sites, and historians. The DMZ provides a buffer between the corporate network and the control system network. The DMZ firewall prevents corporate network users from directly accessing devices on the control system network, but provides a mechanism for them to obtain critical process data for business.

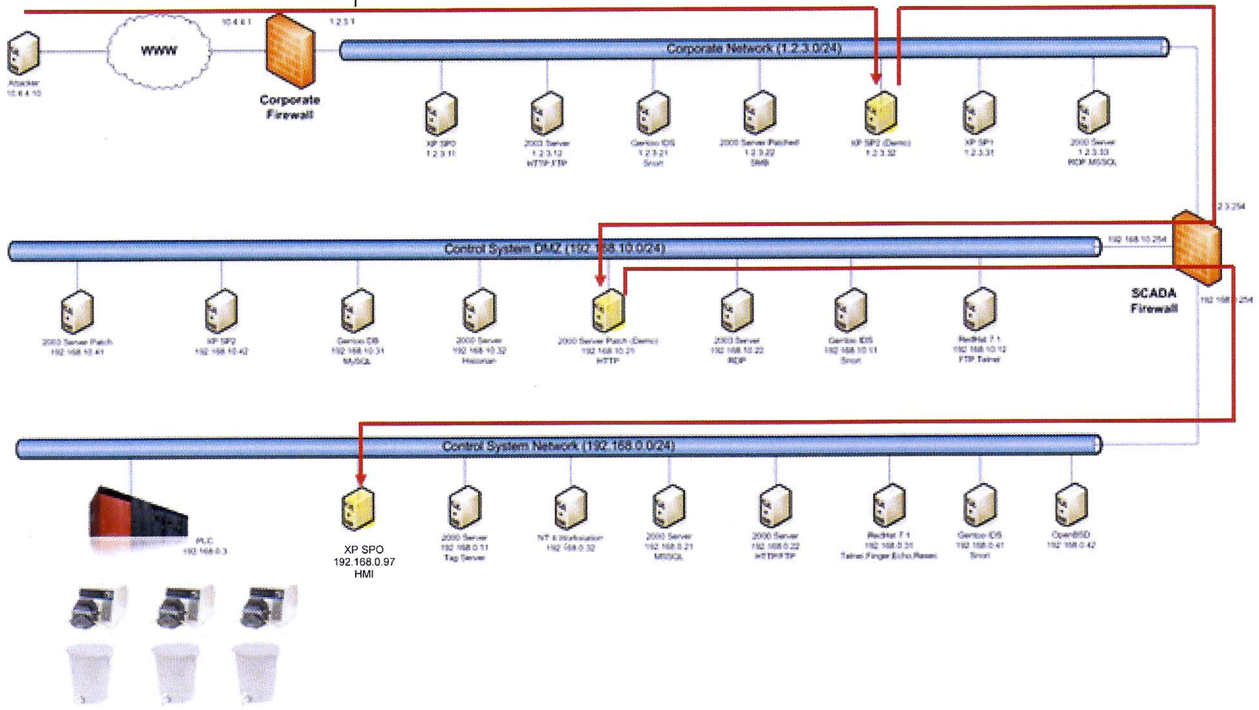
The **control system or SCADA network** consists of servers and workstations found in control systems, including a human-machine interface (HMI), a tag server, and a Programmable Logic Computer (PLC). The HMI is used by operators to manage the process. The tag server exchanges data between the HMI and the PLC. In addition, it translates information into a readable form for the engineer. The PLC on the control network is used to monitor and control a batch mixing process. In industry, this process would mix two process streams and then pass it on to the next process.

The three subnets used in the demonstration have the following IP address range:

Corporate Network	1.2.3.xxx
Control System DMZ	192.168.10.xxx
Control System Network	192.168.0.xxx.

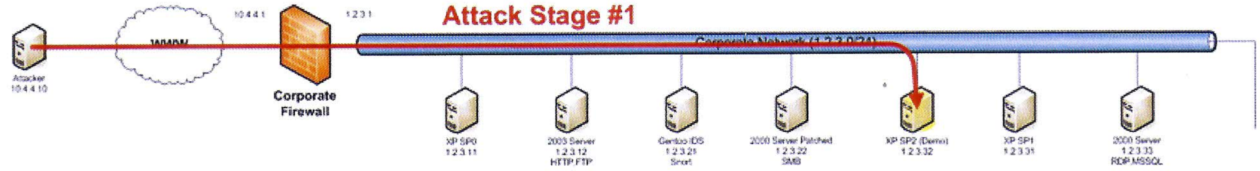
Demo Exploit Path

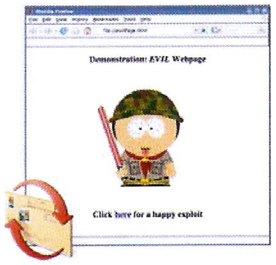
This slide shows the demonstration exploit path through the network. It highlights the workstations that are involved in the attack. The demonstration shows how an attacker can thread his way through the three networks and ultimately gain control of the process control system through the HMI. The attack consists of three stages.



Attack Stage 1 – Internet to Corporate

In the first stage of the attack, an attacker sends a well-crafted email message to a few employees in the company anticipating that at least one will open the embedded link. When the user clicks on the link, the exploit allows the attacker to gain full control of the user's computer.





Demonstration: *EVIL* Webpage

Click here for a happy exploit

Client Side Attack:

Corporate user follows a malicious URL

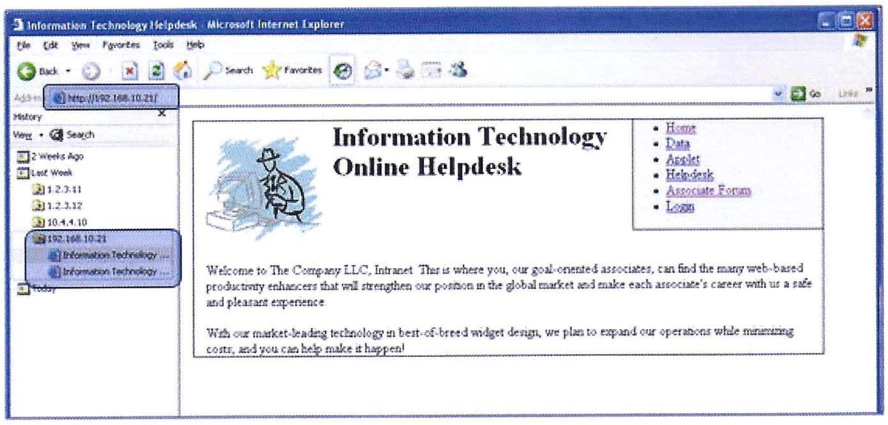
- Social engineering
  - From an e-mail
  - From a suspicious web page.

Triggers a vulnerability on the corp. box

- Exploit payload calls outbound through the firewall to the attacker Internet host
- Attacker gains remote control of the corporate victim

Attack Stage #2 – Reconnaissance

The second stage of the attack starts with reconnaissance of the exploited computer on the corporate network. With a root kit now installed, the attacker can run various system commands and browse system files to gain more information about the networks attached to this particular workstation.


Information Technology Helpdesk - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/
Go Links
History
View Search
2 Weeks Ago
Last Week
1.2.3.11
1.2.3.12
10.4.4.10
192.168.10.21
Information Technology ...
Information Technology ...
Today
Home
Data
Applet
Helpdesk
Associate Forum
Login

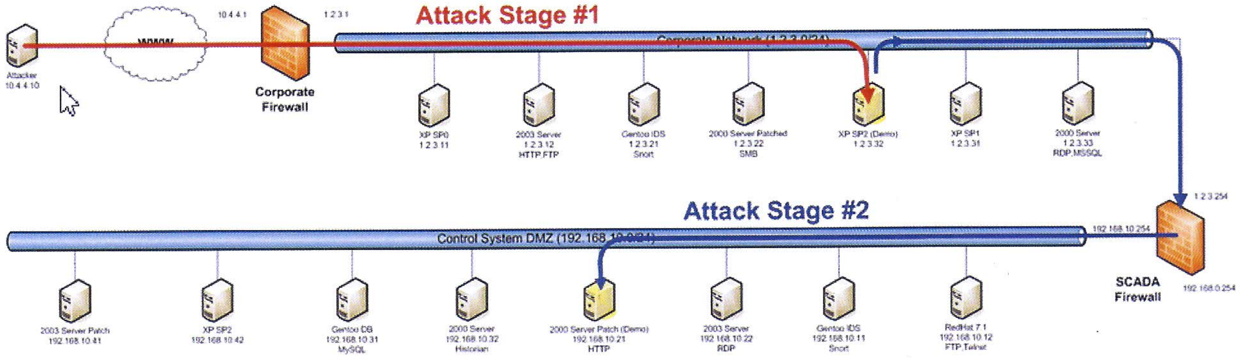
Information Technology Online Helpdesk

Welcome to The Company LLC, Intranet. This is where you, our goal-oriented associates, can find the many web-based productivity enhancers that will strengthen our position in the global market and make each associate's career with us a safe and pleasant experience.

With our market-leading technology in best-of-breed widget design, we plan to expand our operations while minimizing costs, and you can help make it happen!

Victim #1 browser history indicates access to a separate subnet (Victim #1 IP – 1.2.3.32, HTTP IP - 192.168.10.21)

Attack Stage #2 – Corporate to DMZ



Help desk web application allows user to upload arbitrary files:

- Attacker uploads a new PHP file and also an executable rootkit.

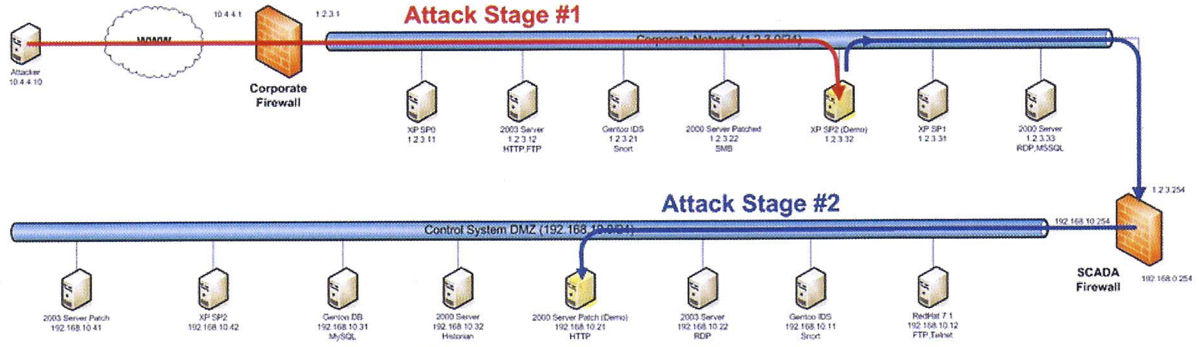
Web site code has an SQL injection problem:

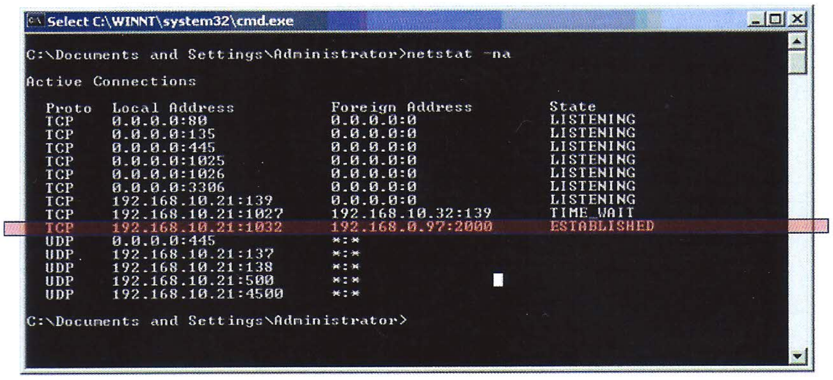
- Provides admin access to the web site (privileged features)
- Attacker makes an HTTP request to an existing admin page and changes the "action" on the URL to include (aka execute) the uploaded PHP page
  - PHP is able to run system commands and launch the rootkit.

Firewall policy:

- Grants **Victim #1** HTTP access to **Victim #2**
- **Victim #2** allowed "any" TCP connection to Internet
- Uploaded rootkit calls back to attacker machine.

Attack Stage #3 – Reconnaissance





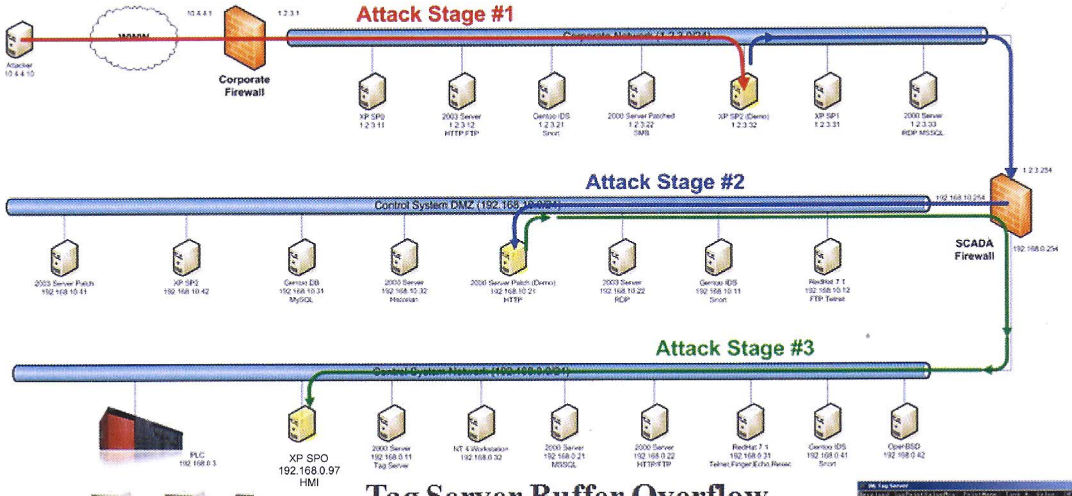
```
C:\Documents and Settings\Administrator>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    192.168.10.21:139      0.0.0.0:0              LISTENING
  TCP    192.168.10.21:1027     192.168.10.32:139      TIME_WAIT
  TCP    192.168.10.21:1032     192.168.0.97:2000      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    192.168.10.21:137      *:*
  UDP    192.168.10.21:138      *:*
  UDP    192.168.10.21:500      *:*
  UDP    192.168.10.21:4500     *:*

C:\Documents and Settings\Administrator>
```

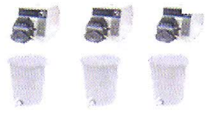
Victim #2

Netstat shows an established connection to a new subnet

Victim #2 IP – 192.168.10.21
Remote Server IP – 192.168.0.97

Attack Stage #3 – DMZ to Control LAN



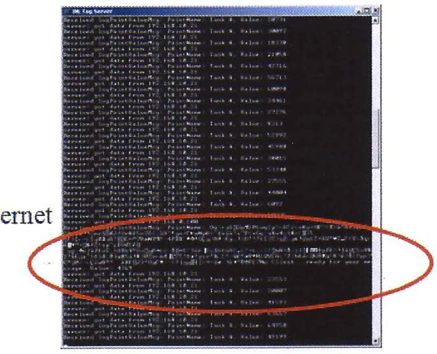


Tag Server Buffer Overflow

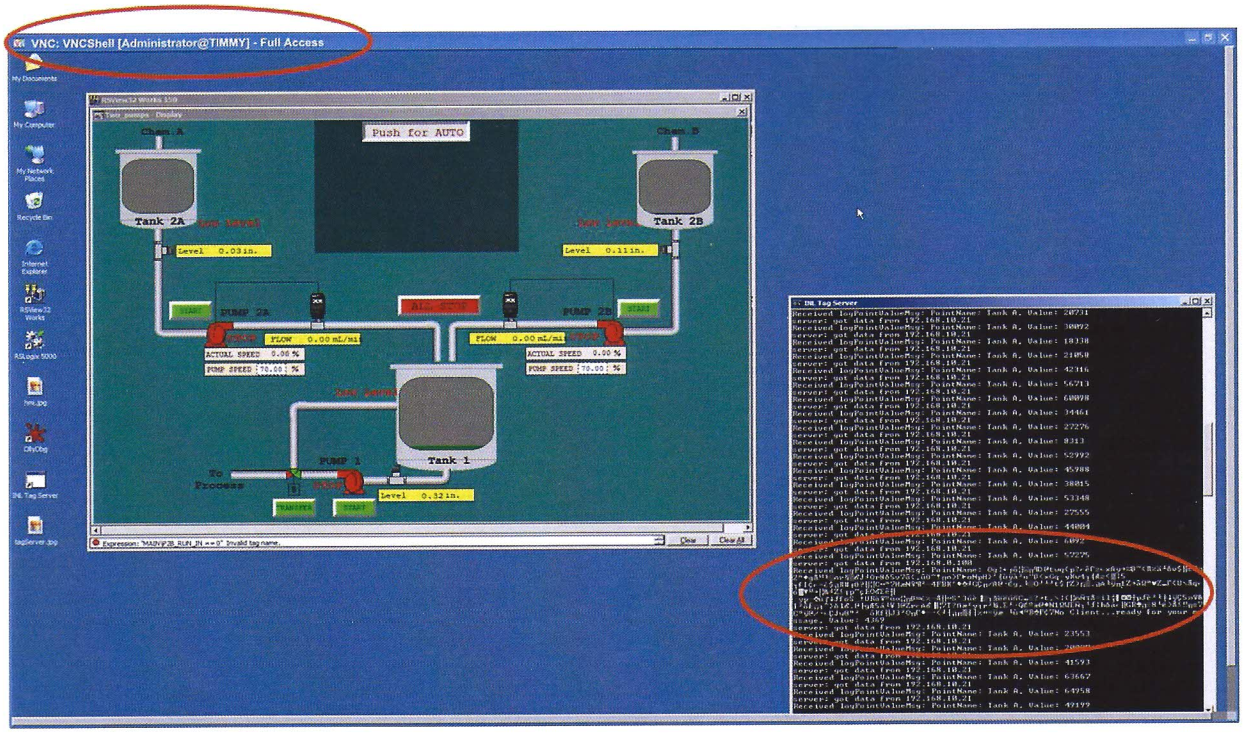
Exploit overflows the point name field

Firewall policy:

- Grants **Victim #2** access to **Victim #3** on Port 2000
- **Victim #3** allowed "any" TCP connection to internet
- Exploit payload calls back to attacker machine



Attack Stage #3 – Pretty Pictures (HMI)

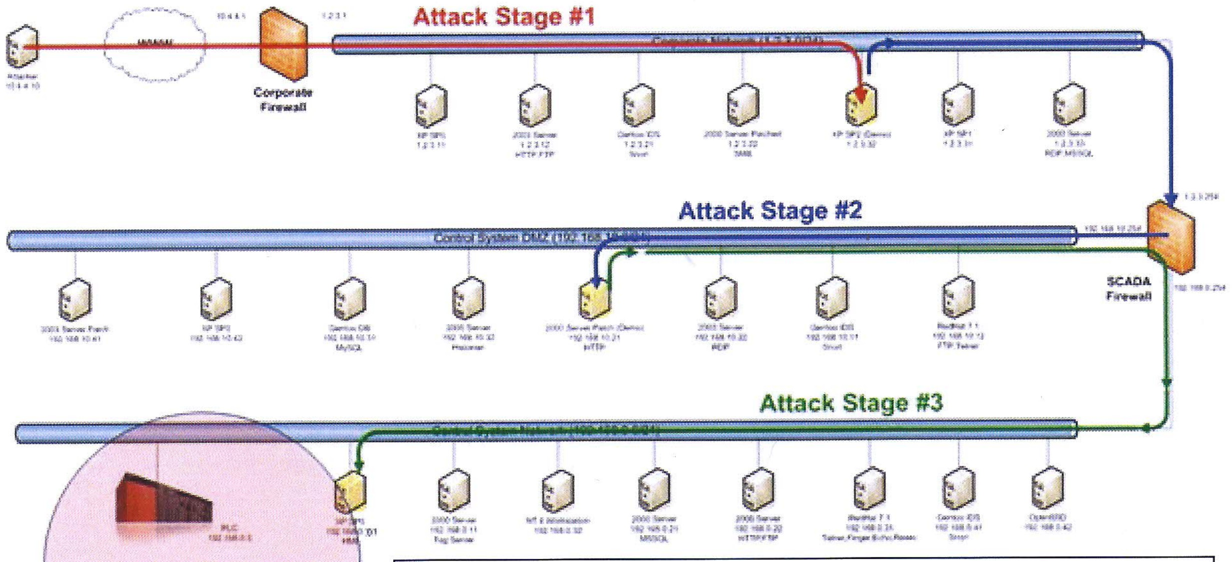


```
Expression: "MAIN\P2B_RUN_IN == 0" Invalid tag name.
```

```
Received logPointValueMsg: PointName: Tank A, Value: 20731
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 30092
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 18338
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 21050
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 42316
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 56713
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 60078
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 34461
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 27276
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 8313
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 52992
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 45788
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 38015
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 53348
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 27555
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 44084
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 6092
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 57275
server: got data from 192.168.0.100
Received logPointValueMsg: PointName: [illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible] Client...ready for your m
ssage. Value: 4369
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 23553
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: [illegible]
server: got data from [illegible]
Received logPointValueMsg: PointName: Tank A, Value: 41593
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 63667
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 64958
server: got data from 192.168.10.21
Received logPointValueMsg: PointName: Tank A, Value: 49199
```

Now that the attacker has access to the HMI, he can control it just like a normal operator of the system. In this case, the HMI is connected to a PLC controlling some process, and the attacker now has full control over that process.

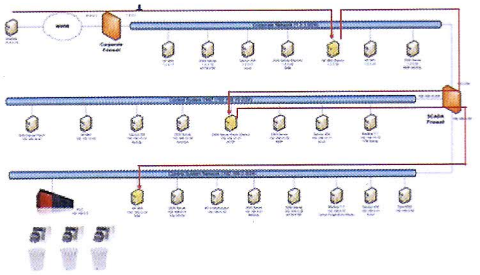
Attack Sends Commands to PLC



- Attacker incrementally expanded attack
- Gained remote control of host inside the control LAN
- Controls the HMI from the Internet.

Homeland Security

Demo Exploit Path



In review, the attacker compromised a workstation on the corporate network using a client side exploit.

→ Attacker then performed some reconnaissance and discovered a new network, which turned out to be the control system DMZ.

→ The attacker then exploited the workstation on the control system DMZ, using SQL injection and flaws in the web application and started the reconnaissance process again.

→ Once again, a new subnet was discovered; this time it was the control system network.

→ A workstation on the control system network was exploited using a zero-day exploit for the tag server, which gave the attacker control over the HMI.

→ Once the attacker had control of the HMI, he was able to manipulate the actual process.

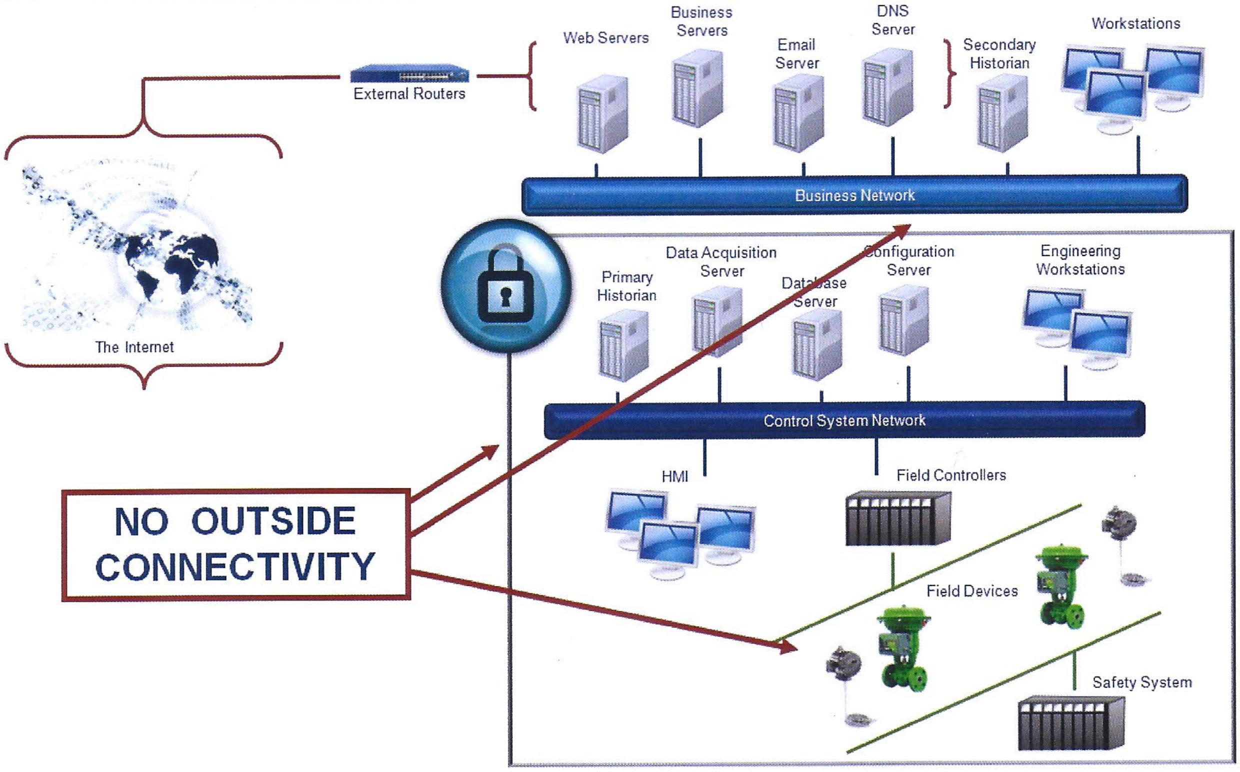
To sum it up, three workstations were compromised using three different types of exploits, and three networks were traversed to gain access to the actual process.

Note: If more of these vulnerabilities had been fixed or patched, this demonstration may not have been successful.

Demo System Vulnerabilities

- Antiquated and/or unpatched
  - Operating systems
  - Services
- Poorly defined firewall policy
- Intrusion detection system (IDS) is underutilized
- Application coding problems
  - Unsafe function usage
  - Logic problems
- Least privileges principle has not been applied to all applications, services, and the network design.

ICS: Traditional Isolation



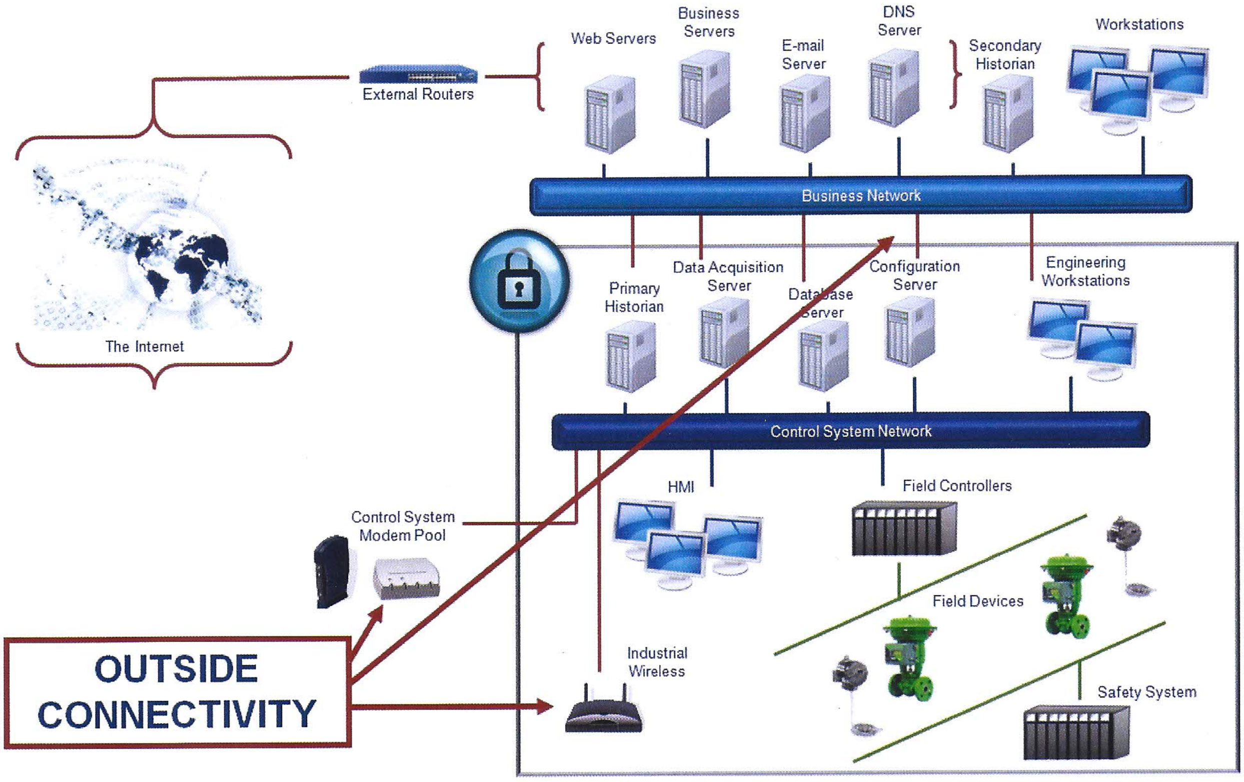
The typical deployment of control systems, regardless of the sector they supported, was based in isolation. The security was done by traditional physical security means, which usually required an employee or operator to have a badge, go past a security guard, and get into a building or facility. Only then would the operator really have access to the control system and the network environment.

This diagram shows many of the traditional corporate IT elements: the standard connectivity to both the Internet and communications infrastructure that would support business operations, and a control systems environment that was not connected to the corporate domain.

From a cybersecurity perspective, this solution presented a fairly low risk, because in many cases there was no access into the operational domain other than physical access.

Traditionally, information relevant to control systems operations was transferred to the corporate domain via paper. Information or reports that needed to get to business operations would be printed out and either faxed to headquarters or a person would physically take the reports to executives and analysts.

ICS: Modern Connectivity



Many organizations establish an electronic security perimeter around their ICSs to protect them from a cyber attack. This perimeter creates a trusted environment within the ICS network. However, we should assume that corporate architectures have been compromised and should treat them as an untrusted network.

An attacker who has a presence on the corporate network uses this trusted relationship to access the control system network. Exploiting this trusted relationship is typically the method an attacker uses to launch a cyber attack on a control system from outside the network.

Some viruses and hostile mobile code are designed to move from network to network by exploiting the simple trust relationship between devices on the corporate and control system networks.

Unlike most IT devices, field controllers (RTUs, PLCs) have limited cybersecurity protection. Field controllers were designed to operate in a trusted environment with reliability and availability being the main objectives.

Modern networks make it possible to access field controllers so technicians can remotely troubleshoot and modify programs. This makes it possible to attack field controllers by intentionally issuing unauthorized set points, modifying the PLC program, setting or resetting the PLC, or creating a denial of service.

Each communication medium has its own vulnerabilities that an attacker can exploit and thus put field controllers at risk.

Wireless (radio, WiFi, microwave)–Insecure wireless access methods provide a significant avenue of attack for adversaries on field controllers. While many radio systems use encryption to secure communications, assessments have shown that many commercial-off-the-shelf solutions provide limited or no security regarding wireless access, or have incorporated security countermeasures that have been publicly broken.

Modems–Over the past several years, the faster and more reliable digital and network circuits have replaced analog communications. Nevertheless, they are still features of legacy architectures and contain a number of vulnerabilities including public dial-up numbers and poor access control that put field controllers at risk.

Private Networks (Lease lines, private lines, fiber optics)–Physical and electronic access, especially lease lines, provides a potential vector an attacker could use to compromise a field controller. These circuits are easy to sabotage, making them unavailable to transmit real-time data.

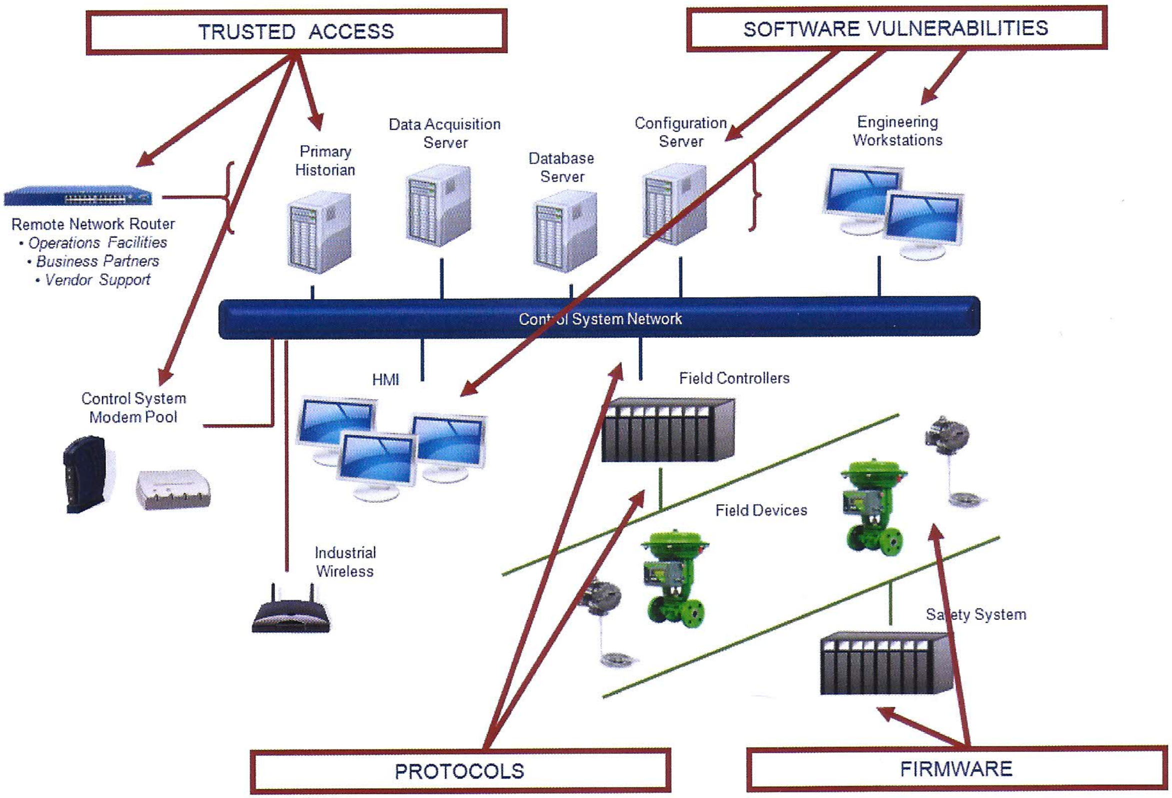
Public Networks (Internet, corporate network)–Essentially the Internet provides a conduit from the outside that an attacker can use to launch an attack.

Remote access provides engineers and technicians the ability to access the control system from an external network. This access extends the electronic perimeter. Typically VPN connections, the primary method of establishing remote communications, if properly installed and configured, are often safer than firewall exceptions. However, because the perimeter has been extended to a remote location, the network engineers do not have as much control over the end device as they do with workstations located locally on company premises.

Inherent Vulnerabilities

Most of the vulnerabilities in ICSs are similar to IT vulnerabilities. Either the vulnerabilities are related IT vulnerabilities or they are related modern networking weaknesses that are integrated with control systems.

Consider a globally popular operating system that is used in mission-critical software applications. Each time an operating system vulnerability is discovered, every ICS that uses that operating system is also vulnerable to that weakness. It is unnerving to think that our nation's ICSs that control and monitor critical infrastructure can share the same types of vulnerabilities as our home computers.



IT and by default ICS vulnerabilities include:

- Hardware & Software
- Firmware & Applications
- Almost any element that correlates to one of the seven layers in the OSI model.

Protocols that were originally developed to exist in an isolated environment are devoid of any inherent security countermeasures.

Review of Session 2

- Connectivity of business and ICS networks increase the exposure of a cyber attack on the ICS.
- Complex systems have many potential points of entry.
- ICS should be monitored for malicious activity.
- Defense-in-depth concepts should be applied to protecting field controllers.